

COMPUTER SYSTEM EQUIPPED WITH USB DEVICE WITH SECURITY FUNCTION

Publication number: JP2003186819 (A)

Publication date: 2003-07-04

Inventor(s): HIRANO ATSUSHI +

Applicant(s): RICOH KK +

Classification:

- international: G06F1/00; G06F13/14; G06F15/00; G06F21/20; G06F1/00; G06F13/14; G06F15/00; G06F21/20; (IPC1-7): G06F1/00; G06F13/14; G06F15/00

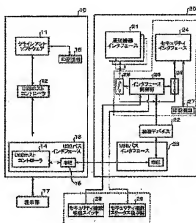
- European:

Application number: JP20010382487 20011217

Priority number(s): JP20010382487 20011217

Abstract of JP 2003186819 (A)

PROBLEM TO BE SOLVED: To provide a computer system equipped with a USB (universal serial bus) device with a security function, comprised of the USB device having a security function and a computer capable of using the USB. ; SOLUTION: A personal computer (PC) 10 has a client software 11 provided with an ID storage part 16, a USB host controller 14 and the like. The USB device 20 has a peripheral equipment interface 21 to achieve an intrinsic function as peripheral equipment, a security interface 24 equipped with an ID storage part 27, an interface control part 25 to control the peripheral equipment interface 21 and the security interface 24, a USB bus interface 23, and the like. By the time when the use of the USB device 20 get authenticated by the PC 10 based on the comparison of IDs of both sides, the state of the security interface 24 becomes to be able to return a descriptor and the state of the peripheral equipment interface 21 becomes not to be able to return a descriptor. ; COPYRIGHT: (C)2003,JPO



Data supplied from the *espacenet* database — Worldwide

(51) Int.Cl. ⁷	識別記号	F I	サーチコード [*] (参考)
G 0 6 F 13/14	3 3 0	G 0 6 F 13/14	3 3 0 C 5 B 0 1 4
1/00	3 7 0	1/00	3 7 0 E 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 C

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号 特願2001-382487(P2001-382487)

(22) 出願日 平成13年12月17日(2001.12.17)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 平野 教

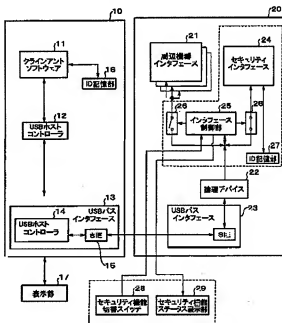
東京都大田区中馬込1丁目3番6号 株式
会社リコー内Fターム(参考) 5B014 EB03 FA05 FB04 GD05 GD22
GD34 GE05 HC04 HC08 HC13
5B085 AE04

(54) 【発明の名称】 セキュリティ機能付きUSB機器を備えたコンピュータシステム

(57) 【要約】

【課題】 セキュリティ機能を有するUSB機器と該USB機器を使用可能なコンピュータからなるセキュリティ機能付きUSB機器を備えたコンピュータシステムを提供する。

【解決手段】 パーソナルコンピュータ(PC)10は、ID記憶部16を備えたクライアントソフトウェア11、USBホストコントローラ14等を有する。USB機器20は、周辺機器としての本来の機能を実現する周辺機器インタフェース21、ID記憶部27を備えたセキュリティインタフェース24、周辺機器インタフェース21とセキュリティインタフェース24を制御するインタフェース制御部25、USBバスインタフェース23等を有する。双方のIDの比較により、USB機器20の使用がPC10により認証されるまで、セキュリティインタフェース24がディスクリプタを返せる状態となり、周辺機器インタフェース21はディスクリプタを返せない状態になる。



【特許請求の範囲】

【請求項1】 USBホストコントローラとIDを保持する記憶手段と認証手段とを有するコンピュータと、周辺機器の機能を実現する周辺機器機能実現手段とセキュリティ機能を実現するセキュリティ機能実現手段と前記周辺機器機能実現手段と前記セキュリティ機能実現手段とを切り替える機能制御手段とIDを保持する記憶手段とを有するUSB機器が接続され、前記USBホストコントローラと前記周辺機器機能実現手段または前記セキュリティ機能実現手段との間で情報の授受を行なうセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記セキュリティ機能実現手段は、前記USB機器に保持されたIDを前記コンピュータに送信し、該認証手段は受信したIDと前記コンピュータに保持されたIDとを比較し、前記USB機器の前記コンピュータでの使用が認証された場合に、前記コンピュータから前記機能制御手段へ前記周辺機器機能実現手段に切り替えるためのコマンドを送信することを特徴とするセキュリティ機能付きUSB機器を備えたコンピュータシステム。

【請求項2】 請求項1に記載のセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記機能制御手段は、前記コンピュータの電力状態が遷移するとき、前記セキュリティ機能実現手段に切り替えることを特徴とするセキュリティ機能付きUSB機器を備えたコンピュータシステム。

【請求項3】 請求項1に記載のセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記コンピュータは、前記認証手段を有効または無効に設定する手段を有することを特徴とするセキュリティ機能付きUSB機器を備えたコンピュータシステム。

【請求項4】 請求項1に記載のセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記USB機器は、前記セキュリティ機能実現手段を有効または無効に切り替える手段を有することを特徴とするセキュリティ機能付きUSB機器を備えたコンピュータシステム。

【請求項5】 請求項4に記載のセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記セキュリティ機能実現手段を有効または無効に切り替える手段は、前記コンピュータでの有効または無効に切り替える操作または前記USB機器に設けられた有効または無効に切り替えるスイッチの操作に応じて、前記コンピュータから送信された前記セキュリティ機能実現手段を有効または無効に切り替えるコマンドにより有効または無効に切り替えられることを特徴とするセキュリティ機能付きUSB機器を備えたコンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、セキュリティ機能

付きUSB機器を備えたコンピュータシステムに関し、より詳細には、コンピュータにUSB機器を接続して使用する際に、お互いに指定されたコンピュータやUSB機器のみ使用可能なセキュリティ機能付きUSB機器を備えたコンピュータシステムに関する。

【0002】

【従来の技術】USB (Universal Serial Bus) は、パーソナルコンピュータの周辺機器の接続規格として、広く普及するようになった。USBの特徴としては以下の(1)～(4)が挙げられ、これらがUSB機器の普及に寄与している。

(1) 様々な種類の機器 (入力機器、オーディオ機器、デジタルカメラ、ビデオカメラ、ネットワーク機器、プリンタ、スキャナ、ストレージ機器など) に対応した規格であること。

(2) 様々な種類の機器が共通のコネクタを用いてパーソナルコンピュータと接続できること。

(3) プラグアンドプレイに対応し、活線挿抜が自由であること。

(4) 1つのホストコントローラに対して最大127台までUSB機器の接続が可能であること。

【0003】このような特徴を有するUSB機器は便利であるが、逆に言えば悪意を持ったユーザが、USB機器を接続し不正な使用を行なうことも容易といことになる。例えば、ストレージ機器を接続してデータの不正な読み書きなどを行なうといった操作を行なうことも容易ということになる。こういった問題点を解決するためには、USB機器に対して何らかのセキュリティ機能が必要である。

【0004】パーソナルコンピュータに接続する機器についてのセキュリティに関する従来技術では、例えば、特開平11-184756号公報 (携帯情報端末におけるセキュリティ制御方法ならびにシステム及び同方法がプログラムされ記録される記憶媒体) というものがある。これは、携帯情報端末内部の不揮発性媒体に記録されている識別番号と接続先のパーソナルコンピュータに記憶されている識別番号との照合をパーソナルコンピュータ側で行い、携帯情報端末側での操作は不要というものである。

【0005】また、特開平7-129736号公報 (ICメモリカード) というものもある。これは、ICメモリカードの中にパスワードを記録した不揮発性媒体と、ユーザがパーソナルコンピュータから入力したパスワードが正しいか否かを判定する回路を持たせるというものである。不正と判定した場合はビジー信号を制御してビジー状態を保持することにより、読み書きを一切できないようにすることを提案している。しかし、USB機器についてのセキュリティについての提案はなかった。

【0006】

【発明が解決しようとする課題】本発明は、上述のごと

き実情に鑑みてなされたもので、セキュリティ機能を有するUSB機器と該USB機器に対応したセキュリティ機能を有するコンピュータからなるセキュリティ機能付きUSB機器を備えたコンピュータシステムを提供することを目的としてなされたものである。

【0007】また、セキュリティ機能を実現する手段が有効に機能するために、この手段が必ず最初にパーソナルコンピュータ側のUSBホストコントローラから認識されるようにし、周辺機器としての本来の機能（ストレージ機器であればストレージの機能）を実現する手段が先に認識されてドライバがロードされ、一時的であっても認証処理より前にUSB機器の使用ができてしまうことを防止することを目的とする。

【0008】更には、セキュリティ機能に対応しているコンピュータに対して通常は接続を許可していないUSB機器の接続を認める設定をも可能とし、例えば、セキュリティ機能に対応していないUSB機器を一時的に使用可能とすることを目的とする。

【0009】更には、セキュリティ機能に対応しているUSB機器を通常は接続を許可していないパーソナルコンピュータへの接続を認める設定をも可能とし、例えば、セキュリティ機能に対応していないパーソナルコンピュータにセキュリティ機能に対応しているUSB機器を一時的に使用可能とすることを目的とする。

【0010】

【課題を解決するための手段】請求項1の発明は、USBホストコントローラとIDを保持する記憶手段と認証手段とを有するコンピュータと、周辺機器の機能を実現する周辺機器機能実現手段とセキュリティ機能を実現するセキュリティ機能実現手段と前記周辺機器機能実現手段と前記セキュリティ機能実現手段とを切り替える機能制御手段とIDを保持する記憶手段とを有するUSB機器が接続され、前記USBホストコントローラと前記周辺機器機能実現手段または前記セキュリティ機能実現手段との間で情報の授受を行うセキュリティ機能付きUSB機器を備えたコンピュータシステムにおいて、前記セキュリティ機能実現手段は、前記USB機器に保持されたIDを前記コンピュータに送信し、該認証手段は受信したIDと前記コンピュータに保持されたIDとを比較し、前記USB機器の前記コンピュータでの使用が認証された場合に、前記コンピュータから前記機能制御手段へ前記周辺機器機能実現手段に切り替えるためのコマンドを送信することを特徴としたものである。

【0011】請求項2の発明は、請求項1の発明において、前記機能制御手段は、前記コンピュータの電力状態が遷移するとき、前記セキュリティ機能実現手段に切り替えることを特徴としたものである。

【0012】請求項3の発明は、請求項1の発明において、前記コンピュータは、前記認証手段を有効または無効に設定する手段を有することを特徴としたものであ

る。

【0013】請求項4の発明は、請求項1の発明において、前記USB機器は、前記セキュリティ機能実現手段を有効または無効に切り替える手段を有することを特徴としたものである。

【0014】請求項5の発明は、請求項4の発明において、前記セキュリティ機能実現手段を有効または無効に切り替える手段は、前記コンピュータでの有効または無効に切り替える操作または前記USB機器に設けられた有効または無効に切り替えるスイッチの操作に応じて、前記コンピュータから送信された前記セキュリティ機能実現手段を有効または無効に切り替えるコマンドにより有効または無効に切り替えられることを特徴としたものである。

【0015】

【発明の実施の形態】以下に、本発明で提案するセキュリティ機能付きUSB機器を備えたコンピュータシステムの実施例について説明する。なお、以下、本発明で説明するセキュリティ機能を持つパーソナルコンピュータをセキュリティ対応PC、セキュリティ機能を持つUSB機器をセキュリティ対応USB機器と呼ぶことにする。

【0016】図1は、本発明の実施例のセキュリティ機能付きUSB機器を備えたコンピュータシステムを示す全体構成図である。コンピュータの構成要素としてUSBの規格では「USBクライアントソフトウェア」、「USBシステムソフトウェア」、「USBホストコントローラ」という3層の論理レイヤが定義されており、パーソナルコンピュータ10においてそれぞれに従って、クライアントソフトウェア11、USBシステムソフトウェア12、USBバスインタフェース13内のUSBホストコントローラ14を有する。更に、USBバスインタフェース13内には、USB機器との通信を行なうSIE (Serial Interface Engine) 15を有し、クライアントソフトウェア11には、ID記憶部16が接続されている。ID記憶部16とは認証用のIDを保持する部分であり、専用の不揮発性メディアを用意してIDを書き込んでおく方法、System BIOSのROMの一部の領域を確保して書き込んでおく方法、オペレーティングシステムやデータファイルが存在するハードディスクにIDを書き込んでおくといった実現方法が考えられる。また、パーソナルコンピュータ10は、表示部17を備えている。表示部17とは、例えば、CRTモニタなどである。

【0017】コンピュータに接続される周辺機器の構成要素としてUSBの規格では「ファンクション」、「USB論理デバイス」、「USBバスインタフェース」という3層の論理レイヤが定義されており、USB機器20においてもそれぞれに従って周辺機器インタフェース（周辺機器の本来の機能を実現する手段）21、論理デバ

ス22、S1EからなるUSBバスインタフェース23を有する。なお、ファンクションとは、インタフェースが複数集合したものであり、インタフェースとは、USBの規格では論理的な機能ことであり、こでも同様の意味を持つものとして用いる。例えば、USBプリンタにおいて、単方向（印字出力の機能のみ）と双方向の2つのモード（印字出力機能と、紙切れやインク切れのチェックなどステータスの読み出し機能）を持つ場合を考えると、このプリンタは、単方向モード、双方向モードという2つのインタフェースがあるといえる。また、論理デバイスとはエンドポイントの集まりである。そして、エンドポイントとは一種のFIFO（First in First out）型のバッファメモリである。例えば、USBプリンタでは、単方向モードには印刷機能にエンドポイントが1つ、双方向モード用には印刷機能とステータス読み出し機能にエンドポイントが1つずつあるということになる。

【0018】更に、USB機器20は、セキュリティインタフェース（セキュリティ機能を実現する手段）24と周辺機器インタフェース21を制御するインタフェース制御部（機能制御手段）25を有する。インタフェース制御部25は、スイッチ26を操作して、周辺機器インタフェース21とセキュリティインタフェース24を切り替えて、一方をディスクリプタを返せる状態に設定し、他方をディスクリプタを返せない状態に設定できる。セキュリティインタフェース24は、認証用のIDを保持する不揮発性メディアからなるID記憶部27が設けられている。また、USB機器20には、セキュリティ機能切替スイッチ28とセキュリティ機能ステータス表示部29が備えられている。このセキュリティ機能切り替えスイッチ28とは、USB機器20のセキュリティ機能を有効または無効に切り替えるためのものであり、現在セキュリティ機能が有効か無効かがセキュリティ機能ステータス表示部29に表示される。

【0019】なお、ディスクリプタとは、プラグアンドプレイの機能をサポートするために、USBの規格で規定された、USBホストコントローラにおいてUSB機器のインタフェースに応じた最適なドライバがロードされるためにUSB機器からコンピュータに返すUSB機器のインタフェースの基本情報のことである。

【0020】以下、パーソナルコンピュータ10側でのセキュリティ対応/未対応、USB機器20側でのセキュリティ対応/未対応の、各々の場合の組み合わせについて組み合わせパターン1～パターン3の2において説明する。

【0021】組み合わせパターン1：セキュリティ対応PC10にセキュリティ対応USB機器20を接続する場合について説明する（請求項1、2）。図2は、本発明におけるセキュリティ機能付きコンピュータの状態遷移を説明するための図である。USB機器20をセキュ

リティ対応PC10に接続することにより、以下の処理が行われる。USBホストコントローラ14がUSB機器20を認識すると（S1）、デバイスパワーステータスを設定する。USB機器20がバスパワータイプのUSB機器である場合は、このときにUSB機器20に電源が入る（S2）。次いで、セキュリティインタフェース24のみがディスクリプタを返せるように初期設定する（S3）。外部電源を使うUSB機器であれば電源投入時の初期設定がこの状態となるようにしてもよい。

【0022】パーソナルコンピュータ10からUSB機器20へインタフェース制御部25の有無を確認するコマンドを送出して（S4）、USB機器20はインタフェース制御部の有無を示す値を返し（S5）、パーソナルコンピュータ10は戻り値を取得し、インタフェース制御部の有無を判定する（S6）。インタフェース制御部がある場合（S6-Yes）、パーソナルコンピュータから、セキュリティインタフェース24のディスクリプタを要求する（S7）。仮に、パーソナルコンピュータにセキュリティ未対応のUSB機器を接続した場合は、インタフェース制御部がないと判定されるので（S6-No）、使用できないことをユーザに通知して終了する（S21）。これにより接続が認められていないUSB機器の接続を防止することができる。

【0023】USB機器20はセキュリティインタフェース24のディスクリプタを返す（S8）。セキュリティインタフェース24のディスクリプタを取得できた場合（S9-Yes）、パーソナルコンピュータ10からUSB機器20へ認証用のIDを要求する（S10）。USB機器20はID記憶部27内に保持しているIDを返す（S11）。パーソナルコンピュータ10はIDを取得し（S12）、セキュリティインタフェース用のドライバをロードして（S13）、パーソナルコンピュータ内のID記憶部16に保持しているIDと照合して（例えば、両方のIDが一致するか判定して）、認証処理を行なう（S14）。何らかの理由でUSB機器20がセキュリティインタフェース24のディスクリプタを返せなかった場合は（S9-No）、使用できないことをユーザに通知して終了する（S21）。

【0024】認証処理の結果、使用を認めると判断した場合は（S15-Yes）、パーソナルコンピュータ10からインタフェース制御部25にコマンドを送出して（S16）、周辺機器としての本来の機能（例えば、USB接続のストレージ機器でいえばストレージ機能）を実現する周辺機器インタフェース21のディスクリプタを返せるようにする（S17）。すなわち、周辺機器インタフェース21側のスイッチ26を閉じるということになる。パーソナルコンピュータ10から、周辺機器インタフェース21のディスクリプタを要求する（S18）。USB機器20は、周辺機器インタフェース21のディスクリプタを返す（S19）。パーソナルコンピ

ュータ10は周辺機器インタフェース21に応じた適切なドライバを選択しロードする(S20)。これにより周辺機器インタフェース21の使用が可能になる。なお、認証処理の結果、使用を認めないと判断した場合は(S15-No)、使用できないことをユーザに通知して終了する(S21)。

【0025】図2には記載していないが、USB機器20を取外す時と、USB機器20を接続したままの状態であってもパーソナルコンピュータ10のシステムのパワーステート(電力状態)を遷移させる時(シャットダウン、スタンバイ、休止状態)について説明する(請求項2)。この時は、パーソナルコンピュータ10からインタフェース制御部25にコマンドを送出して、周辺機器インタフェース21のディスクリプタは返さないようにし、セキュリティインタフェース24のディスクリプタを返せるような状態にする。これにより、取外したUSB機器20を他のPC(特に、セキュリティ機能に未対応のPC)に接続すると認証処理なしに使用できてしまうという危険性をなくすることができる。USB機器20を再度接続するとき、パーソナルコンピュータ10のパワーステートを復帰させる場合は上述した図2の処理を行うことになる。

【0026】以上に説明したように、本発明では、USB機器にセキュリティ機能を実現する手段と、セキュリティ機能を実現する手段と周辺機器の機能を実現する手段とを切り替える手段と、IDを保持する記憶手段を追加し、パーソナルコンピュータに記憶手段と、IDを保持する記憶手段を備えることで、USB機器を備えたコンピュータシステムにセキュリティ機能を付加し、悪意を持ったユーザの不正使用を防止できる。また、本発明では、接続が認められるまでは、周辺機器としての本来の機能(USBプリンタであればプリンタの機能)のディスクリプタを返さないようにする確実なセキュリティ機能を付加できる。

【0027】組み合わせパターン2:セキュリティ対応PCにセキュリティ未対応USB機器を接続する場合について説明する(請求項3)。図3は、本発明におけるPC側のセキュリティ機能の状態遷移を説明するための図である。セキュリティ対応PC10にセキュリティ未対応USB機器を接続する場合は、下方向の矢印で示すように、PC10側のセキュリティ機能を無効にする。ユーザはPC10上でクライアントソフトウェア11の操作で認証処理を無効にする。これにより、セキュリティ未対応のUSB機器を問題なく使えるようになる。セキュリティ機能を再度有効にするためには、PC10上でのクライアントソフトウェア11の操作で認証処理を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【0028】以上に説明したように、セキュリティ機能を持たないUSB機器を組み合わせパターン1で述べた

セキュリティ機能を有するパーソナルコンピュータに接続したことを検出した場合も、そのまま使用できる。

【0029】組み合わせパターン3の1:セキュリティ未対応PCにセキュリティ対応USB機器20を接続する場合について説明する(請求項4および請求項5)。図4は、本発明におけるUSB機器側のセキュリティ機能の状態遷移を説明するための図である。セキュリティ未対応PCにセキュリティ対応USB機器20を接続する場合は、図4の(パターン3の1)と記載された部分の下方向の矢印で示すように、まず、セキュリティ対応PC10に接続してセキュリティ対応USB機器20のセキュリティ機能を無効した後にセキュリティ対応USB機器20を取り外し、セキュリティ未対応のPCに接続する。

【0030】セキュリティ対応USB機器20に対するセキュリティ機能の無効化では、以下の順に処理を行なう。まず、セキュリティ対応USB機器20をセキュリティ対応PC10に接続する。セキュリティ対応PC10はインタフェース制御部25を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応PC10からセキュリティ機能を有効または無効に切り替えるアプリケーションを起動してインタフェース制御部25へコマンドを送出し、セキュリティインタフェース24を無効にし、下方向の矢印で示すように、セキュリティ機能を無効にする。

【0031】セキュリティ対応USB機器20に対してセキュリティ機能を再度有効にする時は、以下の順に処理を行なう。まず、セキュリティ対応USB機器20をセキュリティ対応PC10に接続する。セキュリティ対応PC10はインタフェース制御部25を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応PC10からセキュリティ機能を有効または無効に切り替えるアプリケーションを起動してインタフェース制御部25へコマンドを送出し、セキュリティインタフェース24を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【0032】以上に説明したように組み合わせパターン1で述べたセキュリティ機能を持つUSB機器をセキュリティ機能を持たないパーソナルコンピュータに接続して使用することが可能になる。

【0033】組み合わせパターン3の2:セキュリティ未対応PCにセキュリティ対応USB機器20を接続する場合について説明する(請求項4および請求項5)。図4の(パターン3の2)と記載された部分の下方向の矢印で示すように、まず、パターン3の1と同様に、セキュリティ対応PC10に接続してセキュリティ対応USB機器20のセキュリティ機能を無効した後にセキュリティ対応USB機器20を取り外し、セキュリティ未対応のPCに接続する。

【0034】セキュリティ対応USB機器20に対する

セキュリティ機能の無効化では以下の順に処理を行なう。まず、セキュリティ対応USB機器20をセキュリティ対応PC10に接続する。セキュリティ対応PC10はインタフェース制御部25を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応PC10からセキュリティ機能切替スイッチ28を操作した結果に応じたコマンドを送信して、セキュリティ機能を無効にし、下方向の矢印で示すように、セキュリティ機能を無効にする。

【0035】セキュリティ対応USB機器20に対してセキュリティ機能を再度有効にする時は、以下の順に処理を行なう。まず、セキュリティ対応USB機器20をセキュリティ対応PC10に接続する。セキュリティ対応PC10はインタフェース制御部25を認識して、セキュリティ機能に対応していることを認識する。セキュリティ対応PC10からセキュリティ機能切替スイッチ28を操作した結果に応じたコマンドを送信して、セキュリティ機能を有効にし、上方向の矢印で示すように、セキュリティ機能を有効にする。

【0036】以上に説明したように、組み合わせパターン1で述べたセキュリティ機能を持つUSB機器をセキュリティ機能を持たないパーソナルコンピュータに接続して使用することが、スイッチを操作するという簡便な操作を行なうことで可能になる。

【0037】

【発明の効果】請求項1の発明の効果

特定のコンピュータに対して特定のUSB機器のみの接続を認め、それ以外のUSB機器の使用を無効にすることができる。これにより、例えば、悪意を持ったユーザが、コンピュータにUSB機器を接続し不正な使用を行なうことを防止することができる。また、複数のユーザが使用するコンピュータを管理する管理者が、接続可能なUSB機器を管理するという目的にも使用できる。

【0038】請求項2の発明の効果

コンピュータの電力状態が遷移するとき、USB機器をセキュリティ機能が有効になった状態とするので、周辺機器としての本来の機能が有効になった状態のUSB機器を、本発明によるセキュリティ機能を持たないパーソナルコンピュータに接続して使用される危険性がなくなるので、USB機器の無断持ち出しや盗難を防止することができる。

【0039】請求項3の発明の効果

本発明のセキュリティ機能を持つパーソナルコンピュ

タの1D認識機能を有効または無効に切り替え可能としたので、本発明によるセキュリティ機能を持つパーソナルコンピュータを本発明によるセキュリティ機能を持たないUSB機器と接続して使用することを一時的に認める場合にも対応することができる。

【0040】請求項4、5の発明の効果

本発明のセキュリティ機能を持つUSB機器のセキュリティ機能を有効または無効に切り替え可能としたので、本発明によるセキュリティ機能を持たないコンピュータと、本発明によるセキュリティ機能を持つUSB機器とを接続して使用することを一時的に認める場合にも対応することができる。特に、請求項5の発明では、コンピュータ側のアプリケーションでの操作によりセキュリティ機能を無効にするので、新たなアプリケーションを追加するという簡便な方法でセキュリティ機能を有効または無効にすることができ、また、USB機器に設けたセキュリティ機能の切り替えスイッチによりセキュリティ機能を無効にするので、コンピュータ側のクライアントアプリケーション上での操作を煩わしいと感じるユーザには、セキュリティ機能を有効または無効にする操作に対する煩わしさを感じさせることがない。

【図面の簡単な説明】

【図1】 本発明の実施例のセキュリティ機能付きUSB機器を備えたコンピュータシステムを示す全体構成図である。

【図2】 本発明におけるセキュリティ機能付きコンピュータの状態遷移を説明するための図である。

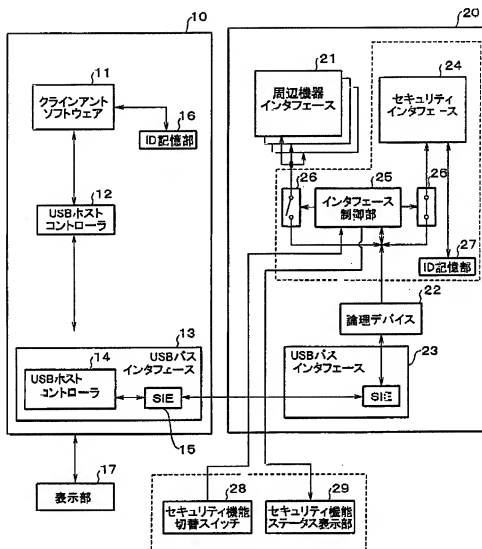
【図3】 本発明におけるPC側のセキュリティ機能の状態遷移を説明するための図である。

【図4】 本発明におけるUSB機器側のセキュリティ機能の状態遷移を説明するための図である。

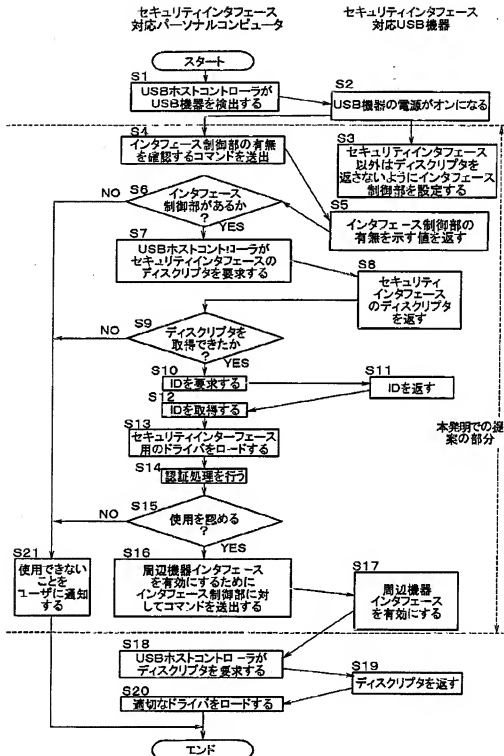
【符号の説明】

10…パーソナルコンピュータ、11…クライアントソフトウェア、12…USBシステムソフトウェア、13…USBバスインタフェース、14…USBホストコントローラ、15…SIE (Serial Interface Engine)、16…ID記憶部、17…表示部、20…USB機器、21…周辺機器インタフェース、22…論理デバイス、23…USBバスインタフェース、24…セキュリティインタフェース、25…インタフェース制御部、26…スイッチ、27…ID記憶部、28…セキュリティ機能切替スイッチ、29…セキュリティ機能ステータス表示部。

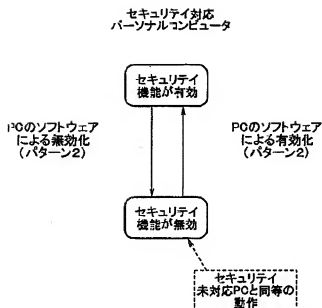
【図1】



【図2】



【図3】



【図4】

